МЕТОДЫ ПРЕДСТАВЛЕНИЯ И ПОИСКА ДОКУМЕНТОВ

METHODS FOR DOCUMENT REPRESENTATION AND RETRIEVAL

КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ПРИ ДОСТАВКЕ ИНФОРМАЦИИ ПОЛЬЗОВАТЕЛЯМ ЭЛЕКТРОННЫХ БИБЛИОТЕК

Кузнецов А.А., Московский государственный технический университет им.Н.Э.Баумана, 105005, Москва, ул.2-я Бауманская, 5, reply@mail.ru

COMPLEX PROTECTION SYSTEM ON TANSFER OF INFORMATION FOR USERS OF ELECTRONIC LIBRARIES

Kuznetsov A.A., Moscow state technical university named after Bauman, 105005, Moscow, st. Second Bauman, 5, reply@mail.ru

The problems of transfer the information for a different level of access for users of electronic libraries are considered in this report.

Появление электронных библиотек с разграниченным доступом пользователей (по степени допуска, размерам оплаты и т.п.) приводит к возникновению задачи ограничения несанкционированного доступа пользователей к их ресурсам [1]. Для решения этой задачи предложена система, состоящая из следующих компонентов:

- Серверная программа для шифрования передаваемой информации одноразовым индивидуальным ключом пользователя [2], выполняющая следующие функции:

1. Регистрация пользователя и определение его уровня допуска;
2. Хранение информации о пользователе и полученных им материалах в базе данных;
3. Пересылка пользователю по открытому каналу программы клиента со встроенными средствами шифровки/дешифровки;
4. Идентификация пользователя при каждом его обращении, проверка его полномочий, отправка ему запрошенной информации в зашифрованном виде и ключа доступа к ней.

- Клиентская программа для расшифровки получаемой информации и отображения ее пользователю, выполняющая следующие функции:

1. Хранение и пересылка идентифицирующей пользователя и саму программу информации;

2. Расшифровка и отображение получаемой из электронной библиотеки информации.

При регистрации пользователя в библиотечной системе ему высылается программа-клиент для расшифровки и отображения получаемой информации. Она передает серверу в зашифрованном виде уникальный идентификатор (имя) пользователя и его пароль.

В базе данных пользователей на сервере создается запись, содержащая его уникальный идентификатор и набор ключей, зашифрованный паролем пользователя, для расшифровки доступной ему информации (информация, относящаяся к одной степени допуска зашифрована одним ключом). Для получения доступа к ресурсам библиотеки программа пользователя сообщает серверу его уникальный идентификатор, пароль и идентификатор запрашиваемого ресурса в зашифрованном виде. Сервер выбирает зашифрованный паролем пользователя ключ для доступа к информации и отправляет его вместе с самой информацией [3].

Получив ответ, программа-клиент расшифровывает ключ своим паролем, а саму информацию этим ключом.

Тройная идентификация полномочий пользователя в предложенной системе по идентификатору пользователя, его паролю и номеру клиентской программы, недоступному пользователю позволяет обеспечить надежную защиту материалов библиотеки от несанкционированного доступа.

Рассмотрим основные этапы организации доставки запрошенной информации пользователям.

Протокол передачи управляющих сообщений:

- Установка связи:

1. Пользователь копирует с сервера или получает по электронной почте открытый ключ для доступа к серверу.
2. Программа-клиент генерирует односеансовый симметричный ключ, шифрует его полученным открытым ключом и отправляет серверу.
3. Сервер возвращает ключ-идентификатор гаммы.

- Обмен информацией:

1. Программа-клиент использует полученный от сервера ключ-идентификатор гаммы для шифрования сообщения. Посылая сообщение, она прикрепляет к нему новое значение ключа-идентификатора гаммы для шифрования ответа сервера.
2. Отвечая, сервер присылает ключ-идентификатор гаммы для шифрования последующего запроса клиента.

Учет пользователей и доставка документов:

- Регистрация пользователя (обмен информацией идет в зашифрованном виде):

1. Программа-клиент отправляет серверу заданный пользователем пароль или встроенный в программу ключ.

2. Сервер создает для пользователя запись в БД со списком ключей, с помощью которых зашифрованы доступные пользователю документы, а также идентификатор для проверки правильности пароля при последующих запросах.

- Изменение полномочий пользователя (обмен информацией идет в зашифрованном виде):

Пользователь присылает свой пароль и, если на сервер поступило или уже имеется (в иерархии условий доступа) соответствующее разрешение, к записи в БД добавляются ключи для доступа к новым документам.

- Доступ к документам:

1. Программа-клиент отправляет серверу заданный пользователем пароль или встроенный в нее ключ и запрос доступа к необходимому документу в зашифрованном с помощью сеансового ключа виде.
2. Сервер выбирает ключ к запрашиваемому документу, а затем отправляет пользователю ключ и сам документ.
3. Программа-клиент расшифровывает паролем пользователя или встроенным в нее ключом полученный от сервера ключ, а с помощью этого ключа расшифровывает сам документ.

Рассмотрим подробнее протоколы установки и поддержания связи в двухключевой криптосистеме, обеспечивающей доставку информации.

Установка связи:

Пользователь получает открытый ключ сервера библиотеки, к документам которой желает осуществить доступ.

Для обеспечения переписки с сервером при каждом новом установлении связи клиент генерирует первичный симметричный ключ (длиной 2048 бит) с помощью которого будут шифроваться последующие сообщения. Этот первичный ключ шифруется с помощью открытого ключа сервера и отправляется ему. Дальнейшие сообщения шифруются методом гаммирования, а для избежания повторения гаммы при каждом последующем запросе/ответе программа клиента/сервера отправляет специальный ключ-идентификатор гаммы, с использованием которого должно быть зашифровано ответное сообщение [4].

Для получения гаммы из первичного ключа формируются 6 ключей, длины которых являются взаимнопростыми числами. Гамма образуется путем циклического суммирования элементов этих ключей. Таким образом, значения элементов гаммы образуются путем суммирования различных сочетаний элементов ключей. В этом случае максимальная длина гаммы равняется произведению длин ключей, использующихся для ее формирования. На рисунках 1 и 2 приведен пример формирования гаммы при использовании 3-х ключей с длинами 5, 3 и 2 байта.

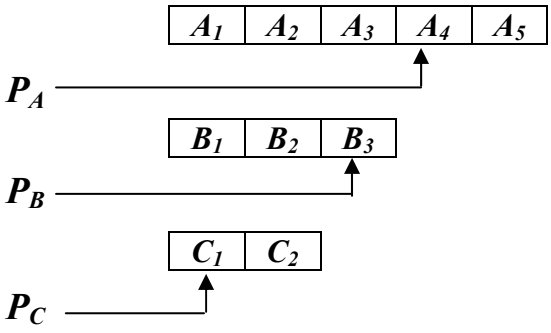

Рис.1. Структура ключей, использующихся для формирования гаммы

	A_1	A_2	A_3	A_4	A_5	A_1	A_2	A_3	A_4	A_5
+	B_1	B_2	B_3	B_1	B_2	B_3	B_1	B_2	B_3	B_1
+	C_1	C_2	C_1	C_2	C_1	C_2	C_1	C_2	C_1	C_2
	K_1	K_2	K_3	K_4	K_5	K_6	K_7	K_8	K_9	K_{10}

Рис.2. Способ формирования гаммы

Здесь: A_i, B_i, C_i – элементы используемых для формирования гаммы ключей, а K_i – получаемые элементы формируемой гаммы.

Ключ-идентификатор гаммы (размером 48 бит) применяется для задания начальных элементов ключей (на рисунке 1 в качестве ключа-идентификатора используются значения P_A, P_B и P_C, – в данном случае его размер составляет 24 бит).

Запрос документа:

После установления связи с сервером программа-клиент посылает ему свой собственный уникальный идентификатор, пароль и идентификатор запрашиваемого документа в зашифрованном с помощью выработанного ключа и присланного сервером ключа-идентификатора гаммы виде. Сервер сверяет хэш-код пароля с хранимым в базе данных хэш-кодом (в случае несовпадения сообщает клиенту об ошибке) и отправляет клиенту ключ для доступа к документу, зашифрованный паролем пользователя, и сам документ, зашифрованный этим ключом [5].

Программа-клиент расшифровывает полученный ключ паролем пользователя или встроенным в нее ключом, расшифровывает присланные документы полученным ключом и отображает этот документ пользователю.

Хранение документов:

Документы хранятся на сервере в базе данных в зашифрованном виде, причем относящиеся к различным уровням доступа документы зашифрованы с помощью различных ключей.

Шифрование документов производится методом гаммирования, причем для избежания повторения гаммы при шифровании каждого документа сохраняется собственный ключ-идентификатор использованной гаммы.

В базе данных пользователей для каждого из них хранится набор ключей к доступным для него документам.

К базе данных предъявлялись следующие требования:

- информация о пользователях должна храниться в зашифрованном с помощью пароля пользователя виде, причем пароль не хранится на сервере, а присылается пользователем при запросах;
- с каждым пользователем должен быть связан список ключей к доступным пользователю документам, зашифрованный с помощью пароля пользователя.
- документы должны храниться в зашифрованном виде;
- документы должны быть разбиты на группы по уровню доступа, причем должна быть обеспечена возможность с помощью одного ключа расшифровать любые документы, относящиеся к одной группе;
- документы должны быть зашифрованы различными участками гаммы.

При этом база данных хранит следующую информацию о пользователях:

- имя пользователя (или его условное имя);
- уникальный идентификатор программы пользователя;
- хэш-код пароля пользователя;
- e-mail пользователя;
- текущий уровень доступа пользователя;
- даты и сроки подключения к библиотеке;
- каталог использованной информации.

На рисунке 3 приведена структурная схема базы данных для хранения документов и информации о пользователях.

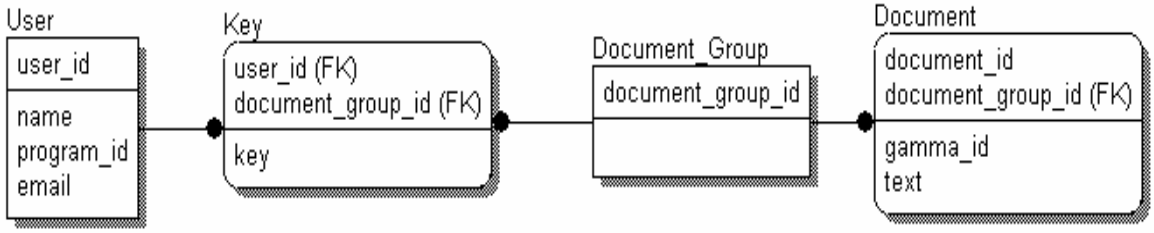

Рис.3. Схема организации базы данных

Здесь: key – ключ для расшифровки документов из группы соответствующего уровня допуска, зашифрованный с помощью пароля пользо-

вателя, gamma_id – ключ-идентификатор гаммы, использующейся для расшифровки документа, text - текст документа, зашифрованный с помощью ключа key.

Таким образом, рассмотренная система позволяет:

- Производить аутентификацию пользователей с помощью пароля либо встроенного ключа программы-клиента, причем так, что даже в случае перехвата текущей переписки между программой-клиентом и сервером полученную информацию нельзя использовать в дальнейшем для получения доступа к информационной базе библиотеки.
- Ограничивать доступ к документам в зависимости от степени допуска пользователей.
- Хранить документы, информацию о пользователях и отчет об их работе на сервере в зашифрованном виде.
- Доставлять документы пользователям в зашифрованном виде, предотвращая тем самым возможность получения содержащейся в документе информации сторонними лицами, перехватывающими передаваемую информацию.
- Не производить специальную перешифровку документов при отправлении их пользователям.

Литература

1. Кузнецов А.А. Основные задачи организации иерархического допуска пользователей электронных библиотек при работе с фондами ограниченного доступа. Тезисы докладов седьмой международной научной конференции «Библиотечное дело-2002», М., 2002г. с.113.
2. Кузнецов А.А. Программа для комплексной криптографической защиты информации с использованием симметричного и асимметричного алгоритмов шифрования. Свидетельство об официальной регистрации программы для ЭВМ №2001611185 от 12.09.2001г.
3. Кузнецов А.А. Способ защиты информации, документов или ценных объектов. Патент России №2182211 от 10.05.2002г.
4. Кузнецов А.А. О граничных условиях применения алгоритмов гаммирования криптосистемы “ХАОС” для защиты информации в технических системах. Тезисы докладов Международной конференции “Информационные средства и технологии”, М., 2001г., т.1. с.94-97.
5. Кузнецов А.А. Определение граничных условий использования хэш-функций при формировании ключей для шифрования массивов информации при передаче сообщений. Тезисы докладов Всероссийской конференции “Методы и технические средства обеспечения безопасности информации”, СПб, 2001 г., с.91-92.